Network Segmentation Using Zones The larger the network, the more difficult it is to protect. A large, unsegmented network presents a large attack surface that can be difficult to manage and protect. Because traffic and applications have access to the entire network, once an attacker gains entry to a network, the attacker can move laterally through the network to access critical data. A large network is also more difficult to monitor and control. Segmenting the network limits an attacker’s ability to move through the network by preventing lateral movement between zones. A security zone is a group of one or more physical or virtual firewall interfaces and the network segments connected to the zone’s interfaces. You control protection for each zone individually so that each zone receives the specific protections it needs. For example, a zone for the finance department may not need to allow all of the applications that a zone for IT allows. To fully protect your network, all traffic must flow through the firewall. Configure Interfaces and Zones to create separate zones for different functional areas such as the internet gateway, sensitive data storage, and business applications, and for different organizational groups such as finance, IT, marketing, and engineering. Wherever there is a logical division of functionality, application usage, or user access privileges, you can create a separate zone to isolate and protect the area and apply the appropriate security policy rules to prevent unnecessary access to data and applications that only one or some groups need to access. The more granular the zones, the greater the visibility and control you have over network traffic. Dividing your network into zones helps to create a Zero Trust architecture that executes a security philosophy of trusting no users, devices, applications, or packets, and verifying everything. The end goal is to create a network that allows access only to the users, devices, and applications that have legitimate business needs, and to deny all other traffic. How to appropriately restrict and permit access to zones depends on the network environment. For example, environments such as semiconductor manufacturing floors or robotic assembly plants, where the workstations control sensitive manufacturing equipment, or highly restricted access areas, may require physical segmentation that permits no access from outside devices (no mobile device access). In environments where users can access the network with mobile devices, enabling User-ID and App-ID in conjunction with segmenting the network into zones ensures that users receive the appropriate access privileges regardless of where they access the network, because access privileges are tied to a user or a user group instead of to a device in one particular zone. The protection requirements for different functional areas and groups may also differ. For example, a zone that handles a large amount of traffic may require different flood protection thresholds than a zone that normally handles less traffic. The ability to define the appropriate protection for each zone is another reason to segment the network. What appropriate protection is depends on your network architecture, what you want to protect, and what traffic you want to permit and deny. PAN-OS® Administrator’s Guide Version 10.2 ©2023 Palo Alto Networks, Inc. 1346Zone Protection and DoS Protection How Do Zones Protect the Network? Zones not only protect your network by segmenting it into smaller, more easily managed areas, zones also protect the network because you can control access to zones and traffic movement between zones. Zones prevent uncontrolled traffic from flowing through the firewall interfaces into your network because firewall interfaces can't process traffic until you assign them to zones. The firewall applies zone protection on ingress interfaces, where traffic enters the firewall in the direction of flow from the originating client to the responding server (c2s), to filter traffic before it enters a zone. The firewall interface type and the zone type (Tap, virtual wire, L2, L3, Tunnel, or External) must match, which helps to protect the network against admitting traffic that doesn't belong in a zone. For example, you can assign an L2 interface to an L2 zone or an L3 interface to an L3 zone, but you can't assign an L2 interface to an L3 zone. In addition, a firewall interface can belong to one zone only. Traffic destined for different zones can't use the same interface, which helps to prevent inappropriate traffic from entering a zone and enables you to configure the protection appropriate for each individual zone. You can connect more than one firewall interface to a zone to increase bandwidth, but each interface can connect to only one zone. After the firewall admits traffic to a zone, traffic flows freely within that zone and is not logged. The more granular you make each zone, the greater the control you have over the traffic that accesses each zone, and the more difficult it is for malware to move laterally across the network between zones. Traffic can't flow between zones unless a security policy rule allows it and the zones are of the same zone type (Tap, virtual wire, L2, L3, Tunnel, or External). For example, a security policy rule can allow traffic between two L3 zones, but not between an L3 zone and an L2 zone. The firewall logs traffic that flows between zones when a security policy rule permits interzone traffic. By default, security policy rules prevent lateral movement of traffic between zones, so malware can't gain access to one zone and then move freely through the network to other targets. Tunnel zones are for non-encrypted tunnels. You can apply different security policy rules to the tunnel content and to the zone of the outer tunnel, as described in the Tunnel Content Inspection Overview. PAN-OS® Administrator's Guide Version 10.2 ©2023 Palo Alto Networks, Inc. 1347Zone Protection and DoS Protection Zone Defense Zone Protection profiles defend zones against flood, reconnaissance, packet-based, and nonIP-protocol-based attacks. DoS Protection profiles used in DoS Protection policy rules defend specific, critical devices against targeted flood and resource-based attacks. A DoS attack overloads the network or targeted critical systems with large amounts of unwanted traffic an attempt to disrupt network services. Plan to defend your network against different types of DoS attacks: • Application-Based Attacks—Target weaknesses in a particular application and try to exhaust its resources so legitimate users can't use it. An example of this is the Slowloris attack. • Protocol-Based Attacks—Also known as state-exhaustion attacks, these attacks target protocol weaknesses. A common example is a SYN flood attack. • Volumetric Attacks—High-volume attacks that attempt to overwhelm the available network resources, especially bandwidth, and bring down the target to prevent legitimate users from accessing those resources. An example of this is a UDP flood attack. There are no default Zone Protection profiles or DoS Protection profiles and DoS Protection policy rules. Configure and apply zone protection based on each zone’s traffic characteristics and configure DoS protection based on the individual critical systems you want to protect in each zone. • Zone Defense Tools • How Do the Zone Defense Tools Work? • Firewall Placement for DoS Protection • Zone Protection Profiles • Packet Buffer Protection • DoS Protection Profiles and Policy Rules Zone Defense Tools Effective defense against DoS attacks requires a layered approach. The first layer of defense should be a dedicated, high-volume DDoS protection device at the internet-facing network perimeter and a perimeter router, switch, or other hardware-based packet drop device with appropriate access control lists (ACLs) to defend against volumetric attacks that the session-based firewall isn’t designed to handle. The firewall adds more granular layers of DoS attack defense and also visibility into application traffic that dedicated DDoS devices don’t provide. Palo Alto Networks firewalls provide four complementary tools to layer in DoS protection for your network zones and critical devices: • Zone Protection profiles defend the ingress zone edge against IP flood attacks, reconnaissance port scans and host sweeps, IP packet-based attacks, and non-IP protocol attacks. The ingress zone is where traffic enters the firewall in the direction of flow from the client to the server (c2s), where the client is the originator of the flow and the server is the responder. Zone Protection profiles provide a second layer of broad defense against DoS attacks, based on the aggregate traffic entering the zone, by limiting the new connections-per-second (CPS) to the PAN-OS® Administrator’s Guide Version 10.2 ©2023 Palo Alto Networks, Inc. 1348Zone Protection and DoS Protection zone. Zone Protection profiles don’t take individual devices (IP addresses) into account because the profiles apply to the aggregate traffic entering the zone. Zone protection profiles defend the network as a session is formed, before the firewall performs DoS Protection policy and Security policy rule lookups, and consume fewer CPU cycles than a DoS Protection policy or Security policy rule lookup. If a Zone Protection profile denies traffic, the firewall doesn’t spend CPU cycles on policy rule lookups. Apply Zone Protection profiles to every zone, both internet-facing and internal. • DoS Protection profiles and policy rules defend specific individual endpoints and resources against flood attacks, especially high-value targets that users access from the internet. While a Zone Protection profile defends the zone from flood attacks, a DoS Protection policy rule with an appropriate DoS Protection profile defends critical individual systems in a zone from targeted flood attacks, providing a granular third layer of defense against DoS attacks. Because the intent of DoS protection is to defend critical devices and because it consumes resources, DoS protection defends only the devices you specify in a DoS Protection policy rule. No other devices are protected. DoS Protection profiles set flood protection thresholds (new CPS limits) for individual devices or groups of devices, resource protection thresholds (session limits for specified endpoints and resources), and whether the profile applies to aggregate or classified traffic. DoS Protection policy rules specify match criteria (source, destination, service ports), the action to take when traffic matches the rule, and the aggregate and classified DoS Protection profiles associated with each rule. Aggregate DoS Protection policy rules apply the CPS thresholds defined in an aggregate DoS

Protection profile to the combined traffic of all the devices that meet the DoS Protection policy rule match criteria. For example, if you configure the aggregate DoS Protection profile to limit the CPS rate to 20,000, the 20,000 CPS limit applies to the aggregate number of connections for the entire group. In this case, one device could receive the majority of the allowed connections. Classified DoS Protection policy rules apply the CPS thresholds defined in a classified DoS Protection profile to each individual device that matches the policy rule. For example, if you configure the classified DoS Protection profile to limit the CPS rate to 4,000, then no device in the group can accept more than 4,000 CPS. A DoS Protection policy can have one aggregate profile and one classified profile. Classified profiles can classify connections by source IP, destination IP, or both. For internet-facing zones, classify by destination IP only because the firewall can’t scale to hold the internet routing table. Apply DoS Protection only to critical devices, especially popular attack targets that users access from the internet, such as web servers and database servers. • For existing sessions, Packet Buffer Protection protects the firewall (and therefore the zone) against single-session DoS attacks that attempt to overwhelm the firewall’s packet buffer, using thresholds and timers to mitigate abusive sessions. You configure Packet Buffer Protection settings globally and apply them per zone. • Security Policy rules affect both the ingress and egress flows of a session. To establish a session, incoming traffic must match an existing Security policy rule. If there is no match, PAN-OS® Administrator’s Guide Version 10.2 ©2023 Palo Alto Networks, Inc. 1349Zone Protection and DoS Protection the firewall discards the packet. A Security policy allows or denies traffic between zones (interzone) and within zones (intrazone) using criteria including zones, IP addresses, users, applications, services, and URL categories. Apply the best practice Vulnerability Protection profile to each Security policy rule to help defend against DoS attacks. The default Security policy rules don’t permit traffic to travel between zones, so you need to configure a Security policy rule if you want to allow interzone traffic. All intrazone traffic is allowed by default. You can configure Security policy rules to match and control intrazone, interzone, or universal (intrazone and interzone) traffic. Zone Protection profiles, DoS Protection profiles and policy rules, and Security policy rules only affect dataplane traffic on the firewall. Traffic originating on the firewall management interface does not cross the dataplane, so the firewall does not match management traffic against these profiles or policy rules. • You can also search the Palo Alto Networks Threat Vault (requires a valid support account and login) for threats by hash, CVE, signature ID, domain name, URL, or IP address. How Do the Zone Defense Tools Work? When a packet arrives at the firewall, the firewall attempts to match the packet to an existing session, based on the ingress zone, egress zone, source IP address, destination IP address, protocol, and application derived from the packet header. If the firewall finds a match, then the packet uses the Security policy rules that already control the session. If the packet doesn’t match an existing session, the firewall uses Zone Protection profiles, DoS Protection profiles and policy rules, and Security policy rules to determine whether to establish a session or discard the packet, and the level of access the packet receives. After traffic passes through your dedicated DDoS device at the internet-facing network edge, the first protection the firewall applies is the broad defense of the Zone Protection profile, if one is attached to the zone. The firewall determines the zone from the interface on which the packet arrives (each interface is assigned to only one zone and all interfaces that carry traffic must belong to a zone). If the Zone Protection profile denies the packet, the firewall discards the packet and saves resources by not needing to look up the DoS Protection policy or Security policy. The firewall applies Zone Protection profiles only to new sessions (packets that do not match an existing session). After the firewall establishes a session, the firewall bypasses the Zone Protection profile lookup for succeeding packets in that session. If the Zone Protection profile doesn’t drop the packet, the second protection the firewall applies is a DoS Protection policy rule. If a Zone Protection profile allows a packet based on the total aggregate amount of traffic going to the zone, a DoS Protection policy rule may deny the packet if it is going to a particular destination or coming from a particular source that has exceeded the flood protection or resource protection settings in the rule’s DoS Protection profile. If the packet matches a DoS Protection policy rule, the firewall applies the rule to the packet. If the rule denies access, the firewall discards the packet and doesn’t perform a Security policy lookup. If the rule allows access, the firewall performs a Security policy lookup. Like the Zone Protection profile, the firewall enforces DoS Protection policy only on new sessions. The third protection the firewall applies is a Security policy lookup, which happens only if the Zone Protection profile and DoS Protection policy rules allow the packet. If the firewall finds no PAN-OS® Administrator’s Guide Version 10.2 ©2023 Palo Alto Networks, Inc. 1350Zone Protection and DoS Protection Security policy rule match for the packet, the firewall discards the packet. If the firewall finds a matching Security policy rule, the firewall applies the rule to the packet. The firewall enforces the Security policy rule on traffic in both directions (c2s and s2c) for the life of the session. Apply the best practice Vulnerability Protection profile to all Security policy rules to help defend against DoS attacks. The fourth protection the firewall applies is packet buffer protection, which you apply globally to protect the device and can also apply individually to zones to prevent single-session DoS attacks that attempt to overwhelm the firewall’s packet buffer. For global protection, the firewall used Random Early Drop (RED) to drop packets (not sessions) when the level of traffic crosses protection thresholds. For per-zone protection, the firewall blocks the source IP address if it violates the packet buffer thresholds. Unlike zone and DoS protection, packet buffer protection applies to existing sessions.